

Elliptic Curve Cryptography Groups IPMEIR IS

Version 1.0

13 May 2010

Prepared By:
National Security Agency
9800 Savage Road
Fort George G. Meade, MD 20755

Table of Contents

1 Introduction.....	3
1.1 Legend.....	3
2 EC Groups for IPMEIR	3
3 Test Vectors	4
3.1 Test Vector: 256-bit Random ECP Group.....	4
3.1.1 Initiator's EC Private Key, EC Public Key and KEi Payload.....	4
3.1.2 Responder's EC Private Key, EC Public Key and KEi Payload	4
3.1.3 Shared Secret	5
3.2 Test Vector: 384-bit Random ECP Group.....	5
3.2.1 Initiator's EC Private Key, EC Public Key and KEi Payload.....	5
3.2.2 Responder's EC Private Key, EC Public Key and KEi Payload	6
3.2.3 Shared Secret	7

List of Tables

Table 1: Legend	3
Table 2: EC Groups for IPMEIR	3
Table 3: 256-bit Random ECP Group - Initiator's EC Private Key	4
Table 4: 256-bit Random ECP Group - Initiator's EC Public Key.....	4
Table 5: 256-bit Random ECP Group - Initiator's KEi Payload	4
Table 6: 256-bit Random ECP Group - Responder's EC Private Key	4
Table 7: 256-bit Random ECP Group - Responder's EC Public Key	5
Table 8: 256-bit Random ECP Group - Responder's KEr Payload.....	5
Table 9: 256-bit Random ECP Group - Shared Secret	5
Table 10: 384-bit Random ECP Group - Initiator's EC Private Key	5
Table 11: 384-bit Random ECP Group - Initiator's EC Public Key.....	6
Table 12: 384-bit Random ECP Group - Initiator's KEi Payload	6
Table 13: 384-bit Random ECP Group - Responder's EC Private Key	6
Table 14: 384-bit Random ECP Group - Responder's EC Public Key	6
Table 15: 384-bit Random ECP Group - Responder's KEr Payload.....	7
Table 16: 384-bit Random ECP Group - Shared Secret	7

1 Introduction

The Internet Protocol Minimum Essential Interoperability Requirements (IPMEIR) Interoperability Specification (IS) mandates support for Elliptic Curve Diffie-Hellman (ECDH), based on the Elliptic Curve (EC) Groups defined in Request For Comments (RFC) 4753 – *ECP Groups for IKE and IKEv2*.

This document is a supplemental technical reference for the IPMEIR IS. Section 2 reiterates the EC Groups detailed in the IPMEIR IS. Section 3 provides test vectors for all EC Groups detailed in the IPMEIR IS.

1.1 Legend

Table 1: Legend

Notation	Definition
du	Initiator's Elliptic Curve Private Key
dv	Responder's Elliptic Curve Private Key
G	Generator
g^ir	Diffie-Hellman Shared Secret
KEi	Key Exchange – Initiator Payload
KEr	Key Exchange – Responder Payload
KEYMAT	Keystream for CHILD_SA keys
n	Prime order of base point G
P	Elliptic Curve Point
Qu	Initiator's Elliptic Curve Public Key
Qv	Responder's Elliptic Curve Public Key
SKEYSEED	Shared Key Seed
xp	Elliptic Curve Point – x coordinate; Diffie-Hellman Shared Secret
xu	Initiator's Elliptic Curve Public Key – x coordinate
xv	Responder's Elliptic Curve Public Key – x coordinate
xy	Elliptic Curve Point – y coordinate
yp	Elliptic Curve Point – y coordinate
yu	Initiator's Elliptic Curve Public Key – y coordinate
yv	Responder's Elliptic Curve Public Key – y coordinate

2 EC Groups for IPMEIR

Table 2: EC Groups for IPMEIR

Diffie-Hellman Group	Transform ID	Reference
256-bit random ECP group	19	- For specific ECP Group characteristics, see RFC 4753 – Section 3.1
384-bit random ECP group	20	- For specific ECP Group characteristics, see RFC 4753 – Section 3.2

3 Test Vectors

3.1 Test Vector: 256-bit Random ECP Group

3.1.1 Initiator's EC Private Key, EC Public Key and KEi Payload

The initiator's EC private key d_u is a randomly selected integer in the interval $[1, n - 1]$.

Table 3: 256-bit Random ECP Group - Initiator's EC Private Key

EC Private Key	Value
d_u	C88F01F5 10D9AC3F 70A292DA A2316DE5 44E9AAB8 AFE84049 C62A9C57 862D1433

The initiator's EC public key Q_u is calculated from $Q_u = (x_u, y_u) = d_u \times G$, where the total length of Q_u is 512-bits (64 bytes).

Table 4: 256-bit Random ECP Group - Initiator's EC Public Key

EC Public Key	Value
Q_u	$Q_u = (x_u, y_u) = d_u \times G$
x_u	DAD0B653 94221CF9 B051E1FE CA5787D0 98DFE637 FC90B9EF 945D0C37 72581180
y_u	5271A046 1CDB8252 D61F1C45 6FA3E59A B1F45B33 ACCF5F58 389E0577 B8990BB3

The initiator's KEi contains the initiator's EC public key Q_u value (Key Exchange Data). Note, the first 8 bytes of the KEi value make up the Key Exchange Payload header. The total length of the KEi payload is 576-bits (72 bytes).

Table 5: 256-bit Random ECP Group - Initiator's KEi Payload

Key Exchange Payload	Value
KEi	00000048 00130000 D12DFB52 89C8D4F8 1208B702 70398C34 2296970A 0BCCB74C 736FC755 4494BF63 56FBF3CA 366CC23E 8157854C 13C58D6A AC23F046 ADA30F83 53E74F33 039872AB

3.1.2 Responder's EC Private Key, EC Public Key and KEi Payload

The responder's EC private key d_v is a randomly selected integer in the interval $[1, n - 1]$.

Table 6: 256-bit Random ECP Group - Responder's EC Private Key

EC Private Key	Value
d_v	C6EF9C5D 78AE012A 011164AC B397CE20 88685D8F 06BF9BE0 B283AB46 476BEE53

The responder's EC public key Q_v is calculated from $Q_v = (x_v, y_v) = d_v \times G$, where the total length of Q_v is 512-bits (64 bytes).

Table 7: 256-bit Random ECP Group - Responder's EC Public Key

EC Public Key	Value
Q_v	$Q_v = (x_v, y_v) = d_v \times G$
x_v	D12DFB52 89C8D4F8 1208B702 70398C34 2296970A 0BCCB74C 736FC755 4494BF63
y_v	56FBF3CA 366CC23E 8157854C 13C58D6A AC23F046 ADA30F83 53E74F33 039872AB

The responder's K_{ER} contains the responder's EC public key Q_v value (Key Exchange Data). Note, the first 8 bytes of the K_{ER} value make up the Key Exchange Payload header. The total length of the K_{ER} payload is 576-bits (72 bytes).

Table 8: 256-bit Random ECP Group - Responder's KER Payload

Key Exchange Payload	Value
K_{ER}	00000048 00130000 D12DFB52 89C8D4F8 1208B702 70398C34 2296970A 0BCCB74C 736FC755 4494BF63 56FBF3CA 366CC23E 8157854C 13C58D6A AC23F046 ADA30F83 53E74F33 039872AB

3.1.3 Shared Secret

The Shared Secret is derived from $P = (x_p, y_p)$ where x_p is the Shared Secret. For the initiator, P is computed from $P = d_u \times Q_v$. For the responder, P is computed from $P = d_v \times Q_u$. The g^{uir} value is the Shared Secret x_p value – g^{uir} is used to calculate SKEYSEED for newly created/rekeyed IKE_SAs and is used to calculate KEYMAT for newly created/rekeyed CHILD_SAs when perfect forward secrecy is desired. The total length of the x_p is 256-bits (32 bytes).

Table 9: 256-bit Random ECP Group - Shared Secret

Shared Secret	Value
x_p	$P = (x_p, y_p)$
x_p	D6840F6B 42F6EDAF D13116E0 E1256520 2FEF8E9E CE7DCE03 812464D0 4B9442DE

3.2 Test Vector: 384-bit Random ECP Group

3.2.1 Initiator's EC Private Key, EC Public Key and KEi Payload

The initiator's EC private key d_u is a randomly selected integer in the interval $[1, n - 1]$.

Table 10: 384-bit Random ECP Group - Initiator's EC Private Key

EC Private Key	Value

du	7633385A B4E8DEB5 DEB53277 D5B782DC 3DEDDBEE4 50538071 84E545B9 931DE55B 85E1D619 653BE5F0 0D679EE0 DA3B757F
----	---

The initiator's EC public key Qu is calculated from $Qu = (xu, yu) = du \times G$, where the total length of Qu is 768-bits (96 bytes).

Table 11: 384-bit Random ECP Group - Initiator's EC Public Key

EC Public Key	Value
Qu	$Qu = (xu, yu) = du \times G$
xu	ACF409CC C491E539 CCDFCB9E 8777E700 691C84B2 9A527E4D A6047B2C E198A1E5 17CA08A4 965DF270 E21CBBE4 A0F7A0E8
y _u	C2E3C6B9 4CA7EAA0 9EC94D05 20A8D09F 0DEF574D 0430A550 A0453173 D00321E2 27DDBBCF 354B9AA0 761DDA3D 194DA84D

The initiator's KEi contains the initiator's EC public key Qu value (Key Exchange Data). Note, the first 8 bytes of the KEi value make up the Key Exchange Payload header. The total length of the KEi payload is 832-bits (104 bytes).

Table 12: 384-bit Random ECP Group - Initiator's KEi Payload

Key Exchange Payload	Value
KEi	0000008C 00150000 ACF409CC C491E539 CCDFCB9E 8777E700 691C84B2 9A527E4D A6047B2C E198A1E5 17CA08A4 965DF270 E21CBBE4 A0F7A0E8 C2E3C6B9 4CA7EAA0 9EC94D05 20A8D09F 0DEF574D 0430A550 A0453173 D00321E2 27DDBBCF 354B9AA0 761DDA3D 194DA84D

3.2.2 Responder's EC Private Key, EC Public Key and KEi Payload

The responder's EC private key dv is a randomly selected integer in the interval $[1, n - 1]$.

Table 13: 384-bit Random ECP Group - Responder's EC Private Key

EC Private Key	Value
dv	DFFFB8C5 E6372143 5236B0BB 6CADD644 F4B49FC7 516B33A4 5B7D9B3E E2885814 0A8FE520 945149A7 F4FC98CB 4C144FE5

The responder's EC public key Qv is calculated from $Qv = (xv, yv) = dv \times G$, where the total length of Qv is 768-bits (96 bytes).

Table 14: 384-bit Random ECP Group - Responder's EC Public Key

EC Public Key	Value
Qv	$Qv = (xv, yv) = dv \times G$
xv	5D4C025F AF150AFC E56E6803 22711AD4 C0939B30 B442DE2D 091EE030 62185843 E2F2190C B3823CFD 4773A9DC E1AFC99D
yv	BD008A34 E8260A23 71733357 0CFAF3DA FC8D6363 D02B37A2 321D1940 72FCFA74 0012AC00 BC5CD36C A6AB7397 3B896FFD

The responder's KER contains the responder's EC public key Qv value (Key Exchange Data). Note, the first 8 bytes of the KER value make up the Key Exchange Payload header. The total length of the KER payload is 832-bits (104 bytes).

Table 15: 384-bit Random ECP Group - Responder's KER Payload

Key Exchange Payload	Value
KER	0000008C 00150000 5D4C025F AF150AFC E56E6803 22711AD4 C0939B30 B442DE2D 091EE030 62185843 E2F2190C B3823CFD 4773A9DC E1AFC99D BD008A34 E8260A23 71733357 0CFAF3DA FC8D6363 D02B37A2 321D1940 72FCFA74 0012AC00 BC5CD36C A6AB7397 3B896FFD

3.2.3 Shared Secret

The Shared Secret is derived from $P = (x_p, y_p)$ where x_p is the Shared Secret. For the initiator, P is computed from $P = du \times Qv$. For the responder, P is computed from $P = dv \times Qu$. The g^{uir} value is the Shared Secret x_p value – g^{uir} is used to calculate SKEYSEED for newly created/rekeyed IKE_SAs and is used to calculate KEYMAT for newly created/rekeyed CHILD_SAs when perfect forward secrecy is desired. The total length of the x_p is 384-bits (48 bytes).

Table 16: 384-bit Random ECP Group - Shared Secret

Shared Secret	Value
x_p	$P = (x_p, y_p)$
x_p	D1B98C18 920EA115 EDE78A20 9E70D0BA F9BABE74 92928847 8050B82E E269F4BF 6C77C85F E93B1D5F B917F282 C30E20A0